Information below update from Anthem:

Members who may have been impacted by the cyber attack against Anthem should be aware of scam email campaigns targeting current and former members. These scams, designed to capture personal information (known as "phishing") are designed to appear as if they are from a health plan and the emails include a "click here" link for credit monitoring. These emails are NOT from Anthem.
DO NOT click on any links in email.
DO NOT reply to the email or reach out to the senders in any way.
DO NOT supply any information on the website that may open, if you clicked on a link in email.
DO NOT open any attachments that arrive with email.

Anthem is not calling members regarding the cyber attack and they are not asking for credit card information or social security numbers over the phone.
This outreach is from scam artists who are trying to trick consumers into sharing personal data. There is no indication that the scam email campaigns are being conducted by those that committed the cyber attack, or that the information accessed in the attack is being used by the scammers.
Anthem will contact current and former members via mail delivered by the U.S. Postal Service about the cyber attack with specific information on how to enroll in credit monitoring. Affected members will receive free credit monitoring and ID protection services.
For more guidance on recognizing scam email, please visit the FTC Website: http://www.consumer.ftc.gov/articles/0003-phishing.
Anthem has created a dedicated website (www.AnthemFacts.com
) where everyone can access information such as frequently asked questions and answers.